

(A) in paragraph (1)(C), by inserting after “compelled” the following: “, coerced, intimidated, or retaliated against”; and

(B) in paragraph (2), by inserting after “compelled” the following: “, coerced, intimidated, or retaliated against”.

(d) EXPANDING AVAILABILITY OF SUPERVISED RELEASE IN TERRORISM-RELATED JUVENILE PROCEEDINGS.—Section 5037(d) of title 18, United States Code, is amended—

(1) in paragraph (2)—

(A) in the matter preceding subparagraph (A), by striking “may not extend”; and

(B) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii), respectively, and adjusting the margins accordingly;

(C) by inserting before clause (i), as so redesignated, the following:

“(A) except as provided in subparagraph (B), may not extend—”;

(D) in subparagraph (A), as so designated—

(i) in clause (i), as so redesignated, by striking “a term that extends”; and

(ii) in clause (ii), as so redesignated—

(I) by striking “a term that extends”; and

(II) by striking the period at the end and inserting “; or”; and

(E) by adding at the end the following:

“(B) may not extend beyond the date that is 10 years after the date when the juvenile becomes 21 years old if the juvenile—

“(i) is charged with an offense listed in section 2332b(g)(5)(B); and

“(ii) is eligible under section 5032 for a motion to transfer to adult status, but is not transferred to adult status.”;

(2) in paragraph (5), in the fifth sentence, by inserting after “26th birthday,” the following: “in the case of a juvenile described in paragraph (2)(B), no term of official detention may continue beyond the juvenile’s 31st birthday.”; and

(3) in paragraph (6), in the second sentence, by inserting after “26th birthday,” the following: “in the case of a juvenile described in paragraph (2)(B), no term of juvenile delinquent supervision may continue beyond the juvenile’s 31st birthday.”.

(e) EXPANDING USE OF SUPERVISED RELEASE FOR CONVICTED TERRORISTS.—Section 5583(j) of title 18, United States Code, is amended—

(1) by striking “for any offense” and inserting the following: “for—

“(1) any offense”;

(2) by striking the period at the end and inserting “; and”; and

(3) by adding at the end the following:

“(2) an offense under section 371 (relating to conspiracy to commit offense against or defraud the United States), when the charge includes an offense listed in section 2332b(5)(B) as the predicate for the conspiracy, is not more than 10 years.”.

(f) CLARIFYING PROCESS FOR PROTECTING CLASSIFIED INFORMATION UNDER THE CLASSIFIED INFORMATION PROCEDURES ACT.—Section 4 of the Classified Information Procedures Act (18 U.S.C. App.) is amended—

(1) by striking “The court, upon” and inserting the following:

“(a) IN GENERAL.—The court, upon”; and

(2) by adding at the end the following:

“(b) PROCEDURE.—If the United States seeks to delete, withhold, or otherwise obtain other relief under subsection (a) with respect to the discovery of any classified information, the United States may object to the disclosure of such classified information, supported by an ex parte declaration signed by any knowledgeable official of the United States possessing authority to classify such information that sets forth the identifiable damage to the national security that the disclosure of such information reasonably could be expected to cause.”.

(g) CLARIFYING APPLICATION OF CLASSIFIED INFORMATION PROCEDURES ACT IN JUVENILE PROCEEDINGS.—Section 1 of the Classified In-

formation Procedures Act (18 U.S.C. App.) is amended by adding at the end the following:

“(c) In this Act, the terms ‘criminal prosecution’, ‘criminal case’, and ‘criminal proceeding’, and any related terms, include proceedings under chapter 403 of title 18, United States Code.”.

(h) CLARIFYING THAT TERRORISTS MAY QUALIFY FOR TRANSFER TO ADULT STATUS UNDER JUVENILE TRANSFER PROVISION.—

(1) DELINQUENCY PROCEEDINGS IN DISTRICT COURTS; TRANSFER FOR CRIMINAL PROSECUTION.—Section 5032 of title 18, United States Code, is amended—

(A) in the first undesignated paragraph—

(i) by striking “or section 1002(a),” and inserting “section 1002(a),”; and

(ii) by striking “section 922(x) or section 924(b), (g), or (h)” and inserting “or section 922(x), 924(b), (g), or (h), or 2332b(g)(5)(B)”; and

(B) in the fourth undesignated paragraph—

(i) in the first sentence—

(I) by striking “or section 1002(a),” and inserting “section 1002(a),”; and

(II) by striking “or section 922(x) of this title, or in section 924(b), (g), or (h)” and inserting “or section 922(x), 924(b), (g), or (h), or 2332b(g)(5)(B)”; and

(ii) in the second sentence—

(I) by striking “crime of violence is an offense under” and inserting “crime is an offense described in”; and

(II) by inserting “or 2332b(g)(5)(B),” after “1113,”; and

(iii) in the fourth sentence, by striking “(i) or 2275” and inserting “or (i), 2275, or 2332b(g)(5)(B)”.

(2) USE OF JUVENILE RECORDS.—Section 5038 of title 18, United States Code, is amended—

(A) in subsection (d), in the first sentence—

(i) by striking “or section 1001(a),” and inserting “, section 1001(a),”; and

(ii) by inserting “or section 2332b(g)(5)(B) of this title,” after “Controlled Substances Import and Export Act,”; and

(B) in subsection (f)—

(i) by striking “or section 1001(a),” and inserting “, section 1001(a),”; and

(ii) by inserting “or section 2332b(g)(5)(B) of this title,” after “Controlled Substances Import and Export Act,”.

SA 4371. Mr. PORTMAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____ . NATIONAL DEEPIFAKE AND DIGITAL PROVENANCE TASK FORCE.

(a) DEFINITIONS.—In this section:

(1) DIGITAL CONTENT FORGERY.—The term “digital content forgery” means the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.

(2) DIGITAL CONTENT PROVENANCE.—The term “digital content provenance” means the verifiable chronology of the origin and history of a piece of digital content, such as an image, video, audio recording, or electronic document.

(3) ELIGIBLE ENTITY.—The term “eligible entity” means—

(A) a private sector or nonprofit organization; or

(B) an institution of higher education.

(4) INSTITUTION OF HIGHER EDUCATION.—The term “institution of higher education” has the meaning given the term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).

(5) RELEVANT CONGRESSIONAL COMMITTEES.—The term “relevant congressional committees” means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives.

(6) SECRETARY.—The term “Secretary” means the Secretary of Homeland Security.

(7) TASK FORCE.—The term “Task Force” means the National Deepfake and Provenance Task Force established under subsection (b)(1).

(b) ESTABLISHMENT OF TASK FORCE.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Director of the Office of Science and Technology Policy, shall establish a task force, to be known as “the National Deepfake Provenance Task Force”, to—

(A) investigate the feasibility of, and obstacles to, developing and deploying standards and technologies for determining digital content provenance;

(B) propose policy changes to reduce the proliferation and impact of digital content forgeries, such as the adoption of digital content provenance and technology standards; and

(C) serve as a formal mechanism for public and private sector coordination and information sharing to facilitate the creation and implementation of a coordinated plan to address the growing threats posed by digital content forgeries.

(2) MEMBERSHIP.—

(A) CO-CHAIRPERSONS.—The following shall serve as co-chairpersons of the Task Force:

(i) The Secretary or a designee of the Secretary.

(ii) The Director of the Office of Science and Technology Policy or a designee of the Director.

(B) COMPOSITION.—The Task Force shall be composed of 12 members, of whom—

(i) 4 shall be representatives from the Federal Government, including the co-chairpersons of the Task Force;

(ii) 4 shall be representatives from institutions of higher education; and

(iii) 4 shall be representatives from private or nonprofit organizations.

(C) APPOINTMENT.—Not later than 120 days after the date of enactment of this Act, the co-chairpersons of the Task Force shall appoint members to the Task Force in accordance with subparagraph (A) from among technical and legal experts in—

(i) artificial intelligence;

(ii) media manipulation;

(iii) digital forensics;

(iv) secure digital content and delivery;

(v) cryptography;

(vi) privacy;

(vii) civil rights; or

(viii) related subjects.

(D) TERM OF APPOINTMENT.—The term of a member of the Task Force shall end on the date described in subsection (g)(1).

(E) VACANCY.—Any vacancy occurring in the membership of the Task Force shall be filled in the same manner in which the original appointment was made.

(F) EXPENSES FOR NON-FEDERAL MEMBERS.—Members of the Task Force described in clauses (ii) and (iii) of subparagraph (B) shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees under subchapter I of

chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Task Force.

(c) **COORDINATED PLAN.**—

(1) **IN GENERAL.**—The Task Force shall develop a coordinated plan to—

(A) reduce the proliferation and impact of digital content forgeries, including by exploring how the adoption of a digital content provenance standard could assist with reducing the proliferation of digital content forgeries;

(B) develop mechanisms for content creators to—

(i) cryptographically certify the authenticity of original media and non-deceptive manipulations; and

(ii) enable the public to validate the authenticity of original media and non-deceptive manipulations to establish digital content provenance; and

(C) increase the ability of internet companies, journalists, watchdog organizations, other relevant entities, and members of the public to—

(i) meaningfully scrutinize and identify potential digital content forgeries; and

(ii) relay trust and information about digital content provenance to content consumers.

(2) **CONTENTS.**—The plan required under paragraph (1) shall include the following:

(A) A Government-wide research and development agenda to—

(i) improve technologies and systems to detect digital content forgeries; and

(ii) relay information about digital content provenance to content consumers.

(B) An assessment of the feasibility of, and obstacles to, the deployment of technologies and systems to capture, preserve, and display digital content provenance.

(C) An assessment of the feasibility of, and challenges in, distinguishing between—

(i) benign or helpful alterations to digital content; and

(ii) intentionally deceptive or obfuscating alterations to digital content.

(D) A discussion of best practices, including any necessary standards, for the adoption and effective use of technologies and systems to determine digital content provenance and detect digital content forgeries.

(E) Conceptual proposals for necessary research projects and experiments to further develop successful technology to ascertain digital content provenance.

(F) Proposed policy changes, including changes in law, to—

(i) incentivize the adoption of technologies, systems, open standards, or other means to detect digital content forgeries and determine digital content provenance; and

(ii) reduce the incidence, proliferation, and impact of digital content forgeries.

(G) Recommendations for models for public-private partnerships to fight disinformation and reduce digital content forgeries, including partnerships that support and collaborate on—

(i) industry practices and standards for determining digital content provenance;

(ii) digital literacy education campaigns and user-friendly detection tools for the public to reduce the proliferation and impact of disinformation and digital content forgeries;

(iii) industry practices and standards for documenting relevant research and progress in machine learning and related areas; and

(iv) the means and methods for identifying and addressing the technical and financial infrastructure that supports the proliferation of digital content forgeries, such as inauthentic social media accounts and bank accounts.

(H) An assessment of privacy and civil liberties requirements associated with efforts

to deploy technologies and systems to determine digital content provenance or reduce the proliferation of digital content forgeries, including statutory or other proposed policy changes.

(I) A determination of metrics to define the success of—

(i) technologies or systems to detect digital content forgeries;

(ii) technologies or systems to determine digital content provenance; and

(iii) other efforts to reduce the incidence, proliferation, and impact of digital content forgeries.

(d) **CONSULTATIONS.**—In carrying out subsection (c), the Task Force shall consult with the following:

(1) The Director of the National Science Foundation.

(2) The National Academies of Sciences, Engineering, and Medicine.

(3) The Director of the National Institute of Standards and Technology.

(4) The Director of the Defense Advanced Research Projects Agency.

(5) The Director of the Intelligence Advanced Research Projects Activity of the Office of the Director of National Intelligence.

(6) The Secretary of Energy.

(7) The Secretary of Defense.

(8) The Attorney General.

(9) The Secretary of State.

(10) The Federal Trade Commission.

(11) The United States Trade Representative.

(12) Representatives from private industry and nonprofit organizations.

(13) Representatives from institutions of higher education.

(14) Such other individuals as the Task Force considers appropriate.

(e) **STAFF.**—

(1) **IN GENERAL.**—Staff of the Task Force shall be comprised of detailees with expertise in artificial intelligence or related fields from—

(A) the Department of Homeland Security;

(B) the National Institute of Standards and Technology; or

(C) any other Federal agency the co-chairpersons of the Task Force consider appropriate with the consent of the head of the Federal agency.

(2) **OTHER ASSISTANCE.**—

(A) **IN GENERAL.**—The co-chairpersons of the Task Force may enter into an agreement with an eligible entity for the temporary assignment of employees of the eligible entity to the Task Force in accordance with this paragraph.

(B) **APPLICATION OF ETHICS RULES.**—An employee of an eligible entity assigned to the Task Force under subparagraph (A)—

(i) shall be considered a special Government employee for the purpose of Federal law, including—

(I) chapter 11 of title 18, United States Code; and

(II) the Ethics in Government Act of 1978 (5 U.S.C. App.); and

(ii) notwithstanding section 202(a) of title 18, United States Code, may be assigned to the Task Force for a period of not more than 2 years.

(C) **FINANCIAL LIABILITY.**—An agreement entered into with an eligible entity under subparagraph (A) shall require the eligible entity to be responsible for any costs associated with the assignment of an employee to the Task Force.

(D) **TERMINATION.**—The co-chairpersons of the Task Force may terminate the assignment of an employee to the Task Force under subparagraph (A) at any time and for any reason.

(f) **TASK FORCE REPORTS.**—

(1) **INTERIM REPORT.**—

(A) **IN GENERAL.**—Not later than 1 year after the date on which all of the appointments have been made under subsection (b)(2)(C), the Task Force shall submit to the President and the relevant congressional committees the coordinated plan developed under subsection (c)(1) in the form of an interim report containing the findings, conclusions, and recommendations of the Task Force.

(B) **CONTENTS.**—The report required under subparagraph (A) shall include specific recommendations for ways to reduce the proliferation and impact of digital content forgeries, including the deployment of technologies and systems to determine digital content provenance.

(2) **FINAL REPORT.**—Not later than 180 days after the date of the submission of the interim report under paragraph (1)(A), the Task Force shall submit to the President and the relevant congressional committees the coordinated plan developed under subsection (c)(1) in the form of a final report containing the findings, conclusions, and recommendations of the Task Force.

(3) **REQUIREMENTS.**—With respect to each report submitted under this subsection—

(A) the Task Force shall make the report publicly available; and

(B) the report—

(i) shall be produced in an unclassified form; and

(ii) may include a classified annex.

(g) **TERMINATION.**—

(1) **IN GENERAL.**—The Task Force shall terminate on the date that is 90 days after the date on which the Task Force submits the final report under subsection (f)(2).

(2) **RECORDS.**—Upon the termination of the Task Force under paragraph (1), each record of the Task Force shall become a record of the National Archives and Records Administration.

SA 4372. Mr. PORTMAN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. . CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

(a) **IN GENERAL.**—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 451 et seq.) is amended by adding at the end the following new section:

“SEC. 890B. HOMELAND SECURITY CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

“(a) IN GENERAL.—

“(1) RESEARCH AND DEVELOPMENT.—The Secretary is authorized to conduct research and development to—

“(A) identify United States critical domains for economic security and homeland security; and

“(B) evaluate the extent to which disruption, corruption, exploitation, or dysfunction of any of such domain poses a substantial threat to homeland security.

“(2) REQUIREMENTS.—

“(A) RISK ANALYSIS OF CRITICAL DOMAINS.—The research under paragraph (1) shall include a risk analysis of each identified United States critical domain for economic security to determine the degree to which